



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **05120194 A**
(43) Date of publication of application: **18.05.1993**

(51) Int. Cl. **G06F 13/12**
G06F 3/06

(21) Application number: **03282451**
(22) Date of filing: **29.10.1991**

(71) Applicant: **NEC ENG LTD**
(72) Inventor: **IIDA SHOZO**

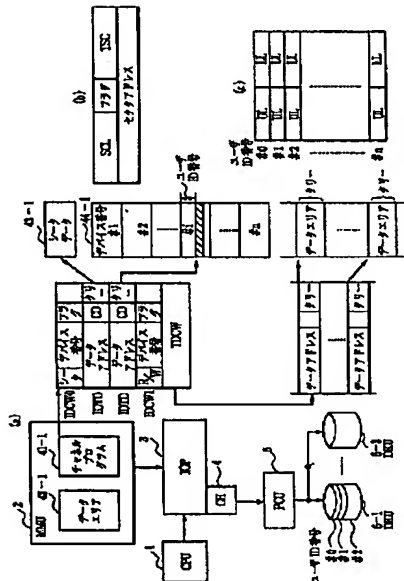
(54) FILE PROTECTIVE SYSTEM

COPYRIGHT: (C)1993,JPO&Japio

(57) Abstract:

PURPOSE: To prevent the file of another user from being destroyed due to the mis-programming of one user.

CONSTITUTION: A CPU 1 issues an I/O request by allocating a user ID number to identify the JOB of an I/O request origin for the I/O request, and generating a channel program 41 to transmit the user ID number to a CH4. A cylinder guard buffer table 44 which allocates a cylinder in which DKUs 6 are continued to each user ID number and consisting of plural cylinder guard buffers representing the maximum value and the minimum value of the cylinder number is provided at every DKU 6. A PCU 5 receives the cylinder guard buffer and seek data 43 in accordance with a device number and the user ID number by the execution of a channel program 41 in an IOP 3, and performs input/output processing under the condition that a sector address is less than LL and also, (sector address + sector count limit) is less than UL.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平5-120194

(43)公開日 平成5年(1993)5月18日

(51)Int.Cl.⁶

G 0 6 F 13/12
3/06

識別記号

3 1 0 Z 7230-5B
3 0 4 H 7165-5B

庁内整理番号

FI

技術表示箇所

審査請求 未請求 請求項の数 5 (全 14 頁)

(21)出願番号 特願平3-282451

(22)出願日 平成3年(1991)10月29日

(71)出願人 000232047

日本電気エンジニアリング株式会社
東京都港区西新橋3丁目20番4号

(72)発明者 飯田 昌三

東京都港区西新橋三丁目20番4号日本電気
エンジニアリング株式会社内

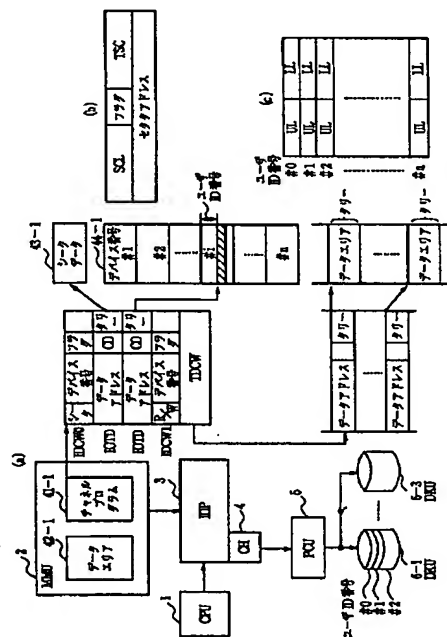
(74)代理人 弁理士 内原 晋

(54)【発明の名称】 ファイル保護方式

(57) 【要約】

【目的】1 ユーザのプログラミングミスによる他のユーザのファイル破壊を防ぐ。

【構成】CPU1がI/O要求に対し、そのI/O要求元のJOBを識別するユーザID番号を割り当て、それをCH4に伝達するチャンネルプログラム41を作成してI/O要求を発行する。各ユーザID番号に対しDKU6の連続したシリンダを割り当てシリンダ番号の最大値と最小値を表示する複数個のシリンダガードバッファから成るシリンダガードバッファテーブル44をDKU6毎に設ける。IOP3におけるチャンネルプログラム41の実行によりPCU5はデバイス番号とユーザID番号に対応するシリンダガードバッファとシークデータ43を受け取り、セクタアドレスがLLより大きく、かつセクタアドレス+セクタカウントリミットがULを越えないことを条件に入出力処理する。



【特許請求の範囲】

【請求項1】 主記憶装置、中央処理装置、チャンネル及び周辺制御装置と入出力装置を含む周辺サブシステムから構成され、前記中央処理装置が入出力命令を実行するとき各入出力要求に対して入出力要求元のプログラムを識別するユーザID番号を割り当てて前記チャンネルに伝達し、前記チャンネルは制御コマンド、デバイス番号、前記主記憶装置上の転送開始データアドレス及び転送語数を含む複数のチャンネルコマンド語から成るチャンネルプログラムを前記主記憶装置から順次読み出して実行することにより前記周辺サブシステムと前記主記憶装置との間の入出力動作を処理する情報処理装置において、前記各ユーザID番号に対し前記主記憶装置上の連続した領域を専有的に割り当ててその領域の先頭アドレスと最終アドレスを保持するメモリガードレジスタを前記ユーザIDの数だけ設け、前記中央処理装置が前記入出力要求を発行したとき前記チャンネルは前記ユーザID番号に対応する前記メモリガードレジスタを選択して前記主記憶装置から前記チャンネルコマンド語を読み出した後このチャンネルコマンド語が指示するデータアドレスが前記メモリガードレジスタに保存された先頭アドレスより上位でありかつ前記データアドレスと前記チャンネルコマンド語が指示する転送語数の加算結果が前記メモリガードレジスタに保持された最終アドレスを越えていないことを条件に前記チャンネルコマンド語で指示された入出力動作を実行することを特徴とするファイル保護方式。

【請求項2】 主記憶装置、中央処理装置、チャンネル及び周辺制御装置と入出力装置を含む周辺サブシステムから構成され、前記中央処理装置が入出力命令を実行するとき各入出力要求に対して入出力要求元のプログラムを識別するユーザID番号を割り当てて前記チャンネルに伝達し、前記チャンネルは制御コマンド、デバイス番号、前記主記憶装置上の転送開始データアドレス及び転送語数を含む複数のチャンネルコマンド語から成るチャンネルプログラムを前記主記憶装置から順次読み出して実行することにより前記周辺サブシステムと前記主記憶装置との間の入出力動作を処理する情報処理装置において、前記各ユーザID番号に対して割り当てられた前記デバイス番号を表示する前記ユーザID番号分のアサインデバイス語から構成されるアサインデバイステーブルを前記チャンネル毎に設け、前記中央処理装置が入出力要求を発行したとき前記チャンネルは前記ユーザID番号及びチャンネル番号に対応する前記アサインデバイス語を選択して前記主記憶装置からチャンネルコマンド語を読み出した後このチャンネルコマンド語で指定されるデバイス番号が前記アサインデバイス語に表示されていることを条件に前記チャンネルコマンド語で指示された入出力動作を実行することを特徴とするファイル保護方式。

【請求項3】 前記中央処理装置が入出力要求を発行したとき前記チャンネルは前記主記憶装置からチャンネルコマ

ンド語を読み出して前記ユーザID番号及びチャンネル番号に対応する前記アサインデバイス語を選択し、前記周辺制御装置は前記チャンネルコマンド語と前記アサインデバイス語を前記チャンネルから受け取りこのチャンネルコマンド語に指定されたデバイス番号が前記アサインデバイス語に表示されていることを条件に前記チャンネルコマンド語で指示された入出力動作を実行することを特徴とする請求項2記載のファイル保護方式。

【請求項4】 主記憶装置、中央処理装置、チャンネル及び周辺制御装置と入出力装置を含む周辺サブシステムから構成され、前記中央処理装置が入出力命令を実行するとき各入出力要求に対して入出力要求元のプログラムを識別するユーザID番号を割り当てて前記チャンネルに伝達し、前記チャンネルは制御コマンド、デバイス番号、前記主記憶装置上の転送開始データアドレス及び転送語数を含む複数のチャンネルコマンド語から成るチャンネルプログラムを前記主記憶装置から順次読み出して実行することにより前記周辺サブシステムと前記主記憶装置との間の入出力動作を処理する情報処理装置において、前記各ユーザID番号に対し前記入出力装置内の連続したシリンダを専有的に割り当ててそのシリンダ番号の最大値と最小値を表示する前記ユーザID番号分のシリンダガードバッファにより構成されるシリンダガードバッファテーブルを設け、前記チャンネルは前記中央処理装置から前記シリンダガードバッファテーブルのロードを指示する入出力要求を受信したとき前記周辺制御装置内に前記シリンダガードバッファテーブルをロードし、更に新たな入出力要求受信により前記チャンネルコマンド語と転送開始セクタアドレスと最大転送セクタ数を含むシークデータ及び前記ユーザID番号を前記周辺制御装置に送出し、前記周辺制御装置は前記ユーザID番号に対応する前記シリンダガードバッファを選択して前記シークデータで指示するセクタアドレスが前記シリンダガードバッファで指示する最小シリンダ番号より大きくかつ前記シークデータで指示するセクタアドレスと最大転送セクタ数の加算結果が前記シリンダガードバッファで指示する最大シリンダ番号を越えていないことを条件に前記チャンネルコマンド語で指示された入出力動作を実行することを特徴とするファイル保護方式。

【請求項5】 前記シリンダガードバッファテーブルを前記入出力装置毎に設け、前記周辺制御装置が入出力要求を発行したとき前記チャンネルは前記主記憶装置から前記チャンネルコマンド語を読み出した後このチャンネルコマンド語に指定されたデバイス番号と前記ユーザID番号に対応する前記シリンダガードバッファを選択し、次に前記周辺制御装置は前記シークデータと前記シリンダガードバッファを前記チャンネルから受け取りそのシークデータで指示するセクタアドレスが前記シリンダガードバッファで指示する最小シリンダ番号より大きくかつ前記シークデータで指示するセクタアドレスと最大転送セク

タ数の加算結果が前記シリンダバッファで指示する最大シリンダ番号を超えていないことを条件に前記チャンネルコマンド語で指示された入出力動作を実行することと特徴とする請求項4記載のファイル保護方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はファイル保護方式に関し、特に情報処理装置における主記憶装置と周辺サブシステム間で転送されるデータを保護するファイル保護方式に関する。

【0002】

【従来の技術】一般にファイルの保護方式は、ファイルの誤用、誤修正及び特定のファイルを一般の人がアクセスすることを防ぐため、1つ1つのファイルを他のファイルと識別するための記号やラベル等をファイルにつけることにより、特定ファイル又はその一部に誤った処理、編集が施されることを防ぐのに使われる。また、上述のようなソフトウェア的な保護方式の他に、1回の入出力で転送されるデータ量の上限を指定して、周辺制御装置がそれを越えてデバイスをアクセスすることを抑止するハードウェア的方式もある。さらに、ファイル保護とは多少性格を異にするが、仮想マシン（VM）方式を採用したシステムにおいて、各システム毎に主記憶を割り当てて1つのシステムが他のシステムのエリアをアクセスしないように入出力処理装置でガードする方式もある。

【0003】図5は従来のファイル保護方式の第1の例を示す情報処理装置のブロック図で、周辺制御装置におけるファイル保護方法を示している。図5において、本例の情報処理装置は中央処理装置（CPU）1と、主記憶装置（MMU）2と、入出力処理装置（IOP）3と、入出力チャンネル（CH）4と、周辺制御装置（PCU）5と、磁気ディスク（DKU）6-1、～6-3とから構成され、IOP3はMMU2上に用意されたチャンネルプログラム51-1を実行することでMMU2とDKU6の間のデータ転送を制御する。IOP3はCPU1からの入出力（I/O）要求を受信すると、チャンネルプログラムの第1語IDCW0をPCU5に送出し、第2語IOTDを実行することでシークデータを送出する。PCU5は図5（b）に示すシークデータ内のセクタカウントリミット（SCL）と転送セクタカウント（TSC）とを比較し、ファイル54に示すようにTSCがSCLより大きいときは次のコマンド（第3語IDCW1）により処理されるデータ転送をSCLの値で終了させる。

【0004】次に、図6は従来のファイル保護方式の第2の例を示す情報処理装置のブロック図で、VM方式により1つのシステムに割り当てられたエリアを他のシステムがアクセスするのを防ぐ方法を示している。図6において、本例の情報処理装置はCPU1と、MMU2

と、IOP3と、CH4と、PCU5と、DKU6-1、～6-3とから構成される。IOP3はMMU2とDKU6-1、～6-3間のデータ転送を行うとき、CPU1からのI/O要求で指定されたシステムID（S-ID）番号をVMIDレジスタ62にセットし、それに対応するメモリガードバッファ63-1をレジスタファイルから読み出して、それをアドレスレジスタ64に保持されているリクエストアドレスと比較してからメモリアccessを行う。本動作はメモリアccessのたびに行われる。図6（b）はメモリガードバッファの内容を示し、UL/LLはそれぞれ1つのシステムに割り当てられたメモリの上限/下限を表す。リクエストアドレス>ULまたはリクエストアドレス<LL（OR回路66の出力が“1”）のときはメモリガードエラーとしてメモリアccessを抑止する。

【0005】

【発明が解決しようとする課題】この従来のファイル保護方式では、ソフトウェア的手段による場合はハードウェア的手段によるガードがないので、ユーザのプログラミング上の転送方向・モードの指定ミス、転送量の指定ミス、更にはデータ転送を実行するかしないか又は転送方向、モード等を特定条件の判定により決定するようなプログラムの論理ミス等の原因で他のユーザのファイルを破壊する可能性がある。

【0006】また、周辺制御装置（PCU）におけるセクタカウントリミットを利用した方式（図5）の場合でも、PCUは各入出力とユーザとの対応を認識できないので、上述と同様にユーザのプログラミング上のミスが原因で他のユーザエリアを破壊する可能性がある。

【0007】さらに、VM方式によるメモリガードの場合（図6）は、ハードウェア的手段を使用しているが、システム間のメモリガードを行うだけで1つのシステム内におけるユーザ間のファイル保護は不可能である。

【0008】本発明の目的は、1つ1つのI/O要求を他のI/Oと識別するためのユーザID番号をI/O要求の中で指定できるようにし、1つのI/O要求で指示するデータ転送がユーザID番号毎に設定されたアクセス可能範囲を越えないようにハードウェアでガードするファイル保護方式を提供することにある。

【0009】

【課題を解決するための手段】第1の発明のファイル保護方式は、主記憶装置、中央処理装置、チャンネル及び周辺制御装置と入出力装置を含む周辺サブシステムから構成され、前記中央処理装置が入出力命令を実行するとき各入出力要求に対して入出力要求元のプログラムを識別するユーザID番号を割り当てて前記チャンネルに伝達し、前記チャンネルは制御コマンド、デバイス番号、前記主記憶装置上の転送開始データアドレス及び転送語数を含む複数個のチャンネルコマンド語から成るチャンネルプログラムを前記主記憶装置から順次読み出して実行するこ

5

とにより前記周辺サブシステムと前記主記憶装置との間の入出力動作を処理する情報処理装置において、前記各ユーザ I D 番号に対し前記主記憶装置上の連続した領域を専有的に割り当ててその領域の先頭アドレスと最終アドレスを保持するメモリガードレジスタを前記ユーザ I D の数だけ設け、前記中央処理装置が前記入出力要求を発行したとき前記チャンネルは前記ユーザ I D 番号に対応する前記メモリガードレジスタを選択して前記主記憶装置から前記チャンネルコマンド語を読み出した後このチャンネルコマンド語が指示するデータアドレスが前記メモリガードレジスタに保存された先頭アドレスより上位でありかつ前記データアドレスと前記チャンネルコマンド語が指示する転送語数の加算結果が前記メモリガードレジスタに保持された最終アドレスを越えていないことを条件に前記チャンネルコマンド語で指示された入出力動作を実行することを特徴とする。

【0010】第2の発明のファイル保護方式は、主記憶装置、中央処理装置、チャンネル及び周辺制御装置と入出力装置を含む周辺サブシステムから構成され、前記中央処理装置が入出力命令を実行するとき各入出力要求に対して入出力要求元のプログラムを識別するユーザ I D 番号を割り当てて前記チャンネルに伝達し、前記チャンネルは制御コマンド、デバイス番号、前記主記憶装置上の転送開始データアドレス及び転送語数を含む複数のチャンネルコマンド語から成るチャンネルプログラムを前記主記憶装置から順次読み出して実行することにより前記周辺サブシステムと前記主記憶装置との間の入出力動作を処理する情報処理装置において、前記各ユーザ I D 番号に対して割り当てられた前記デバイス番号を表示する前記ユーザ I D 番号分のアサインデバイス語から構成されるアサインデバイステーブルを前記チャンネル毎に設け、前記中央処理装置が入出力要求を発行したとき前記チャンネルは前記ユーザ I D 番号及びチャンネル番号に対応する前記アサインデバイス語を選択して前記主記憶装置からチャンネルコマンド語を読み出した後このチャンネルコマンド語で指定されるデバイス番号が前記アサインデバイス語に表示されていることを条件に前記チャンネルコマンド語で指示された入出力動作を実行することを特徴とする。そして、前記中央処理装置が入出力要求を発行したとき前記チャンネルは前記主記憶装置からチャンネルコマンド語を読み出して前記ユーザ I D 番号及びチャンネル番号に対応する前記アサインデバイス語を選択し、前記周辺制御装置は前記チャンネルコマンド語と前記アサインデバイス語を前記チャンネルから受け取りこのチャンネルコマンド語に指定されたデバイス番号が前記アサインデバイス語に表示されていることを条件に前記チャンネルコマンド語で指示された入出力動作を実行してもよい。

【0011】第3の発明のファイル保護方式は、主記憶装置、中央処理装置、チャンネル及び周辺制御装置と入出力装置を含む周辺サブシステムから構成され、前記中央

6

処理装置が入出力命令を実行するとき各入出力要求に対して入出力要求元のプログラムを識別するユーザ I D 番号を割り当てて前記チャンネルに伝達し、前記チャンネルは制御コマンド、デバイス番号、前記主記憶装置上の転送開始データアドレス及び転送語数を含む複数のチャンネルコマンド語から成るチャンネルプログラムを前記主記憶装置から順次読み出して実行することにより前記周辺サブシステムと前記主記憶装置との間の入出力動作を処理する情報処理装置において、前記各ユーザ I D 番号に対し前記入出力装置内の連続したシリンダを専有的に割り当ててそのシリンダ番号の最大値と最小値を表示する前記ユーザ I D 番号分のシリンダガードバッファにより構成されるシリンダガードバッファテーブルを設け、前記チャンネルは前記中央処理装置から前記シリンダガードバッファテーブルのロードを指示する入出力要求を受信したとき前記周辺制御装置内に前記シリンダガードバッファテーブルをロードし、更に新たな入出力要求受信により前記チャンネルコマンド語と転送開始セクタアドレスと最大転送セクタ数を含むシークデータ及び前記ユーザ I D 番号を前記周辺制御装置に送出し、前記周辺制御装置は前記ユーザ I D 番号に対応する前記シリンダガードバッファを選択して前記シークデータで指示するセクタアドレスが前記シリンダガードバッファで指示する最小シリンダ番号より大きくかつ前記シークデータで指示するセクタアドレスと最大転送セクタ数の加算結果が前記シリンダガードバッファで指示する最大シリンダ番号を越えていないことを条件に前記チャンネルコマンド語で指示された入出力動作を実行することを特徴とする。そして、前記シリンダガードバッファテーブルを前記入出力装置毎に設け、前記周辺制御装置が入出力要求を発行したとき前記チャンネルは前記主記憶装置から前記チャンネルコマンド語を読み出した後このチャンネルコマンド語に指定されたデバイス番号と前記ユーザ I D 番号に対応する前記シリンダガードバッファを選択し、次に前記周辺制御装置は前記シークデータと前記シリンダガードバッファを前記チャンネルから受け取りそのシークデータで指示するセクタアドレスが前記シリンダガードバッファで指示する最小シリンダ番号より大きくかつ前記シークデータで指示するセクタアドレスと最大転送セクタ数の加算結果が前記シリンダガードバッファで指示する最大シリンダ番号を越えていないことを条件に前記チャンネルコマンド語で指示された入出力動作を実行してもよい。

【0012】

【実施例】次に、本発明について図面を参照して説明する。図1(a)は本発明のファイル保護方式の第1の実施例を示す情報処理装置のブロック図である。

【0013】図1(a)において図5と同じ略号を用いた装置は第1の従来例における装置と同じ名称の装置であり、本実施例はCPU1と、MMU2と、IOP3と、CH4と、PCU5と、DKU6-1、～6-3と

を備え、7はMMU2内のメモリ領域を示す。図1 (b)は同図(a)におけるメモリガードバッファの1語のフォーマットを示す図である。

【0014】CPU1はIOP3とインタフェースを持ち、IOP3は配下に複数のCH4を持ち、MMU2とPCU5を接続する。DKU6-1、~6-3はPCU5の下に芋づる式につながっている。CPU1は演算機能を有し、I/O命令を検出するとIOP3にI/O要求を送出する。IOP3は内部にユーザIDレジスタ8とメモリガードバッファ9-1とアドレスレジスタ10と比較回路11とOR回路12を有し、CPU1からのI/O要求を受けてMMU2とDKU6-1、~6-3の間のデータ転送を処理する。PCU5はCH4からコマンドを受け取ってDKU6-1、~6-3のハードウェア(HW)動作制御及びI/O動作を多重制御する。

【0015】続いて本第1の実施例におけるファイル保護の動作について説明する。CPU1はプログラム実行中にI/O命令を検出すると、そのI/O命令に対し主記憶上の特定エリアを割り当て、そのエリアの上位アドレス(UL)と下位アドレス(LL)からなるメモリガードバッファを作成する。更に、上記のエリアを指定するためのユーザID番号を割り当ててIOP3にI/O要求を送出する。IOP3はI/O要求を受け付けるとメモリガードバッファとユーザID番号をCPU1から引き取ってユーザID番号をユーザIDレジスタ8にセットし、ユーザIDレジスタ8をアドレスとしてメモリガードバッファ9-1にUL、LLの値を格納する。次に、IOP3はCPU1から指示されたI/O要求に従って入出力動作を行う際にすべてのメモリリクエストに対して以下のチェックを行う。IOP3はメモリリクエストアドレスをアドレスレジスタ10にセットし、リクエスト送出時にユーザIDレジスタ8によりメモリガードバッファ9-1内の(UL、LL)を読み出し、比較回路11でリクエストアドレス>UL、リクエストアドレス<LLのチェックを行う。どちらの条件も成立しない場合はアドレスレジスタ10が指示するMMU2上のデータをリード/ライトし、どちらかの条件が成立した場合は割り当てられたエリアを越えたアクセスと判断し、入出力動作を中断してメモリガードエラーをオペレーティングシステム(OS)に通知する。このようにして、CPU1からのI/O要求に従って行われる入出力動作において、そのI/O要求に割り当てられたMMU2上のエリアの上限/下限を示す(UL、LL)値を使って入出力動作が上記エリアを越えて行われないようにIOP3でガードすることができる(請求項1記載の動作)。

【0016】次に、図2(a)は本発明の第2の実施例を示す情報処理装置のブロック図である。本実施例では説明を簡単にするために、1つのチャンネルだけに注目して説明する。

【0017】第1の実施例と同様、本実施例はCPU1、MMU2、IOP3、CH4、PCU5、DKU6-1、~6-3を備え、21-1はチャンネルプログラム、22はコマンド(IDCW)、23-1はアサインデバイステーブル、26、28はコマンド(IDCW)、27、29はアサインデバイスワードで、CPU1からDKU6-1、~6-3までの接続関係、構成も図1と同様である。チャンネルプログラム21-1は複数のチャンネルコマンド語(CCW)から構成され、CCWはPCU5に指示するコマンド、デバイス番号及びフラグ部とMMU2上のデータアドレス、転送データ量等を含む。

【0018】図2(b)は同図(a)におけるチャンネルプログラムの構成例を示す図で、特にIDCWはコマンド、IOTDはデータアドレス、TDCWは次のCCWのアドレスを指す。

【0019】図2(c)は同図(a)におけるアサインデバイステーブルのフォーマット例を示す図で、ユーザID番号分のアサインデバイスワード27、29で構成されかつCH毎に設けられ、アサインデバイスワードはCH毎にI/O要求に割り当てられたユーザID番号で利用できるデバイスを指定し、デバイス番号に対応するビットが“1”のとき、そのデバイスが使用可能であることを示す。

【0020】続いて第2の実施例におけるファイル保護の動作について説明する。CPU1はシステム立ち上げ時にデバイス番号と所有ユーザとの対応情報を外部から取り込んでアサインデバイステーブル23-1をMMU2上に作成する。次にCPU1はプログラム実行中にI/O命令を検出するとそのI/O命令に対しユーザID番号を割り当て、MMU2上にチャンネルプログラム21-1を作成してIOP3にI/O要求を送出する。このとき、ユーザID番号はチャンネルプログラム21-1内のIDCW22に設定される。次にIOP3はCPU1からのI/O要求を受信するとチャンネルプログラム21-1をMMU2から1語ずつ読み出して実行する。

【0021】IOP3はIDCW22を取り込み(25-1)、IDCW22に指定されたユーザID番号に対応するアサインデバイスワードを取り込む(24-1)。IOP3内に取り込んだIDCW26とアサインデバイスワード27を使ってIDCW26内のデバイス番号に対応するアサインデバイスワード27のビットをチェックし、“1”ならば指定されたDKUを使って入出力動作を行い、“0”ならば不正デバイス指定エラーをOSに通知して入出力動作を終了する(請求項2記載の動作)。

【0022】IOP3はIDCW22をPCU5に送出し(25-2)、IDCW22内のユーザID番号に対応するアサインデバイスワードもPCU5に送出する(24-2)。PCU5はIOP3から受け取ったID

CW28とアサインデバイスワード29を使ってIDCW28内のデバイス番号に対応するアサインデバイスワード29のビットをチェックし、“1”ならば指定されたDKUを使って入出力動作を行い、“0”ならばIOP3に対して不正デバイス指定エラーの終了報告を行う。IOP3はそのエラーをOSに通知して入出力動作を終了する。このようにして、CPU1からのI/O要求に従って行われる入出力動作において、そのI/O要求で指定されたデバイスがそのI/O要求に割り当てられたユーザID番号でアクセス可能か否かのチェックをIOP3又はPCU5内部で行い、各ユーザが他のユーザ所有のデバイスをアクセスできないようにガードすることができる(請求項3記載の動作)。

【0023】次に、図3(a)は本発明の第3の実施例を示す情報処理装置のブロック図である。本実施例は第1の実施例と同様、CPU1、MMU2、IOP3、CH4、PCU5、DKU6-1、~6-3を備え、31-1はチャンネルプログラム、32-1はシークデータ、33-1はシリンダガードバッファテーブル、36はコマンド(IDCW)、37はシリンダガードバッファで、図3(b)、(c)、(d)はそれぞれ同図(a)におけるチャンネルプログラム、シークデータ、シリンダガードバッファテーブルのフォーマット例を示す図である。CPU1からDKU6-1、~6-3までの接続関係及び構成は第1の実施例と同様である。

【0024】シリンダガードバッファテーブル33-1は図2(d)に示すようにユーザID番号分のシリンダガードバッファから構成され、シリンダガードバッファはI/O要求に割り当てられたユーザID番号でアクセス可能なシリンダ番号の最大値(UL)の最小値(LL)を指定する。シークデータ32-1は図3(b)に示すようにセクタカウトリミット、フラグ、転送セクタカウント及びセクタアドレスから成り、セクタカウトリミットはチャンネルプログラム31-2内のIDCW1の処理により転送されるデータの最大値を示し、転送セクタカウントはIDCW1の処理により転送されるデータ量を示し、セクタアドレスはIDCW1の処理により行われるデータ転送の開始セクタアドレスを示す。

【0025】続いて本第3の実施例におけるファイル保護の動作について説明する。CPU1はシステム立上げ時にシリンダガードバッファテーブル33-1をMMU2上に作成し、シリンダガードバッファテーブル33-1をPCU5にロードするためのI/O要求をIOP3に発行することによりシリンダガードバッファテーブル33-1をPCU5内に格納する(34)。次にCPU1がプログラム実行中にI/O命令を検出するとそのI/O命令にユーザID番号を割り当て、MMU2上にチャンネルプログラム31-1を作成してIOP3にI/O要求を送出する。このときユーザID番号は図3(b)に示すチャンネルプログラム内のIDCW0に設定され

る。次にIOP3はCPU1からI/O要求を受信するとチャンネルプログラム31-1の先頭IDCWを読み出してPCU5へ送出する(35)。また、次のIOTDの実行によりシークデータ32-1もPCU5に送出する。

【0026】PCU5はIOP3から受け取ったIDCW36で指示されたユーザID番号に対応するシリンダガードバッファ37を選択し、IOP3から受け取ったシークデータを使ってセクタアドレス+セクタカウトリミット>UL、セクタアドレス<LLのチェックを行い、どちらの条件も成立しなければ入出力動作を継続し、どちらかの条件が成立した場合は指定されたユーザID番号に対応するアクセス可能なシリンダを越えたと判断してIOP3にシリンダガードエラーの終了報告を行う。IOP3はこのエラーをOSに通知して入出力動作を終了する。このようにして、CPU1からのI/O要求に従って行われる入出力動作において、入出力動作が上記I/O要求に割り当てられたユーザID番号でアクセスできるシリンダ番号を越えて行われなようにPCU5でガードすることができる(請求項1記載の動作)。

【0027】次に、図4(a)は本発明の第4の実施例を示す情報処理装置のブロック図である。本実施例は第1の実施例と同様、CPU1、MMU2、IOP3、CH4、PCU5、DKU6-1、~6-3を備え、41-1はチャンネルプログラム、42-1はデータエリア、43-1はシークデータ、44-1はシリンダガードバッファテーブルで、図4(b)及び(c)はそれぞれ同図(a)におけるシークデータ及び1デバイス当りのシリンダガードバッファテーブルのフォーマット例を示す図である。CPU1からDKU6-1、~6-3までの接続関係及び構成は第1の実施例と同様である。チャンネルプログラムはPCU5に対するコマンドを含むCCW(IDCW0/1)、データ転送を指示するCCW(IOTP、IOTD)及び次に実行するCCWアドレスを指すTDCWから構成されている。IOTPは次にデータ転送指示のCCWが続くことを意味し(データチェン)、IOTDは本DCWの実行で入出力動作が終了することを意味する。また、IOTPはシークデータをPCU5へ転送することを指示し、IOTDはシリンダガードバッファテーブル内のシリンダガードバッファ1語をPCU5へ転送することを指示する。シークデータ43-1の内容は図4(b)に示した通りである。シリンダガードバッファテーブル44-1は図4(c)に示すようにユーザID番号分のシリンダガードバッファから成るテーブルがデバイス毎に用意され、シリンダガードバッファには、I/O要求に割り当てられたユーザ番号でアクセス可能なシリンダ番号の最大値(UL)と最小値(LL)が記述されている。

【0028】続いて本第4の実施例におけるファイル保

護の動作について説明する。CPU1はシステム立上げ時に1つのDKU内のシリンダをユーザID番号の数に分割し、MMU2上にシリンダガードバッファテーブルを個々のDKU毎に作成する。シリンダの分割はDKU毎に独立に行われるため、同じユーザID番号に対応するシリンダガードバッファの(UL, LL)値でもDKU毎に異なる。次にCPU1はプログラム実行中にI/O命令を検出すると、I/O命令にユーザID番号を割り当ててMMU2上にチャンネルプログラム41-1とシークデータ43-1を作成する。このときチャンネルプログラム41-1のIOTDはIDCW0で指定するデバイス番号に対応するシリンダガードバッファテーブル44-1内で上記のユーザID番号に対応するシリンダガードバッファを指す。IOP3は上記I/O要求を受け付けると、チャンネルプログラム41-2のIDCW0をPCU5に送出し、続いてIOTP, IOTDを実行することによりPCU5にシークデータ43-1とIOTDが指示するシリンダガードバッファを送出する。

【0029】PCU5はIOP3からシークデータ43-1とシリンダガードバッファを受け取るとセクタアドレス+セクタカウントリミット>UL, セクタアドレス<LLのチェックを行い、どちらの条件も成立しない場合はIDCW0で指定されたデバイスを使って入出力動作を行い、どちらかの条件が成立する場合にはIDCW0で指示されたデバイスにおいてI/O要求に割り当てられたユーザID番号でアクセス可能なシリンダを越えたと判断してPCU5はIOP3にシリンダガードエラーの終了報告を行う。IOP3はこのエラーをOSに通知して入出力動作を終了する。このようにして、CPU1からのI/O要求に従って行われる入出力動作において、データ転送が上記I/O要求に割り当てられたユーザID番号でアクセスできる(デバイス毎に独立に決定された)シリンダ番号を越えて行われなようにPCU5でガードすることができる(請求項5記載の動作)。

【0030】

【発明の効果】以上説明したように本発明は、以下のような効果を有する。

【0031】第1に、CPUがIOPに送出するI/O要求にユーザID番号を割り当て、入出力動作が各ユーザID番号に対して割り当てられた主メモリ領域内で行われるようにIOPでガードすることにより、ユーザのプログラミングのミスが原因で他のユーザが使用している主メモリ上のデータを破壊することがなくなる。また、通信処理装置を介して複数の端末とホスト間で通信を行うシステムにおいて各回線で行うデータ送受が回線毎に割り当てられた主メモリ領域内で行われるようにIOPでガードするので、通信処理装置の故障が原因で他の回線用のメモリエリアを破壊することを防ぐことができる。

【0032】第2に、CPUがIOPに送出するI/O

要求にユーザID番号を割り当て、ユーザID番号毎に使用可能なデバイスを規定することにより、1ユーザが他のユーザ所有のデバイスをアクセスすることを防ぎ、誤って他のユーザのファイルを破壊することを防止することができる。また、デバイス番号チェックをPCUでチェックすることにより、IOPの負担及びハードウェア量を軽減して同様の効果を得ることができる。

【0033】第3に、ユーザID番号毎に磁気ディスク内でアクセス可能なシリンダ番号を規定することにより、他のユーザが使用するシリンダ上のデータ(ファイル)を破壊することを防ぎ、複数のユーザが1つのディスクを共用し、かつ各ユーザがあたかも1つのディスク装置の中に個人専用の小単位のディスクを専有しているかのように運用することができる。また、ユーザID番号毎に磁気ディスク内でアクセス可能なシリンダ番号を各ディスク独立に規定することにより、システムに接続された磁気ディスクの1つ1つを複数ユーザに分割することができ、かつシリンダを分割する単位(サイズ)が同じユーザID番号でもデバイス番号によって変化させることができる。さらに、1ユーザがプログラミングミス等の原因により他のユーザのシリンダ(ファイル)を破壊することを防ぐことができる。

【図面の簡単な説明】

【図1】(a)は本発明のファイル保護方式の第1の実施例を示す情報処理装置のブロック図、(b)は同図(a)におけるメモリガードバッファの1語のフォーマット例を示す図である。

【図2】(a)は本発明の第2の実施例を示す情報処理装置のブロック図、(b)及び(c)はそれぞれ同図(a)におけるチャンネルプログラムの構成例を示す図及びアサインデバイステーブルのフォーマット例を示す図である。

【図3】(a)は本発明の第3の実施例を示す情報処理装置のブロック図、(b)、(c)、(d)はそれぞれ同図(a)におけるチャンネルプログラム、シークデータ、シリンダガードバッファテーブルのフォーマット例を示す図である。

【図4】(a)は本発明の第4の実施例を示す情報処理装置のブロック図、(b)及び(c)はそれぞれ同図(a)におけるシークデータ及び1デバイス当りのシリンダガードバッファテーブルのフォーマット例を示す図である。

【図5】従来のファイル保護方式の第1の例を示す情報処理装置のブロック図である。

【図6】従来のファイル保護方式の第2の例を示す情報処理装置のブロック図である。

【符号の説明】

- 1 中央処理装置(CPU)
- 2 主記憶装置(MMU)
- 3 入出力処理装置(IOP)

(8)

特開平5-120194

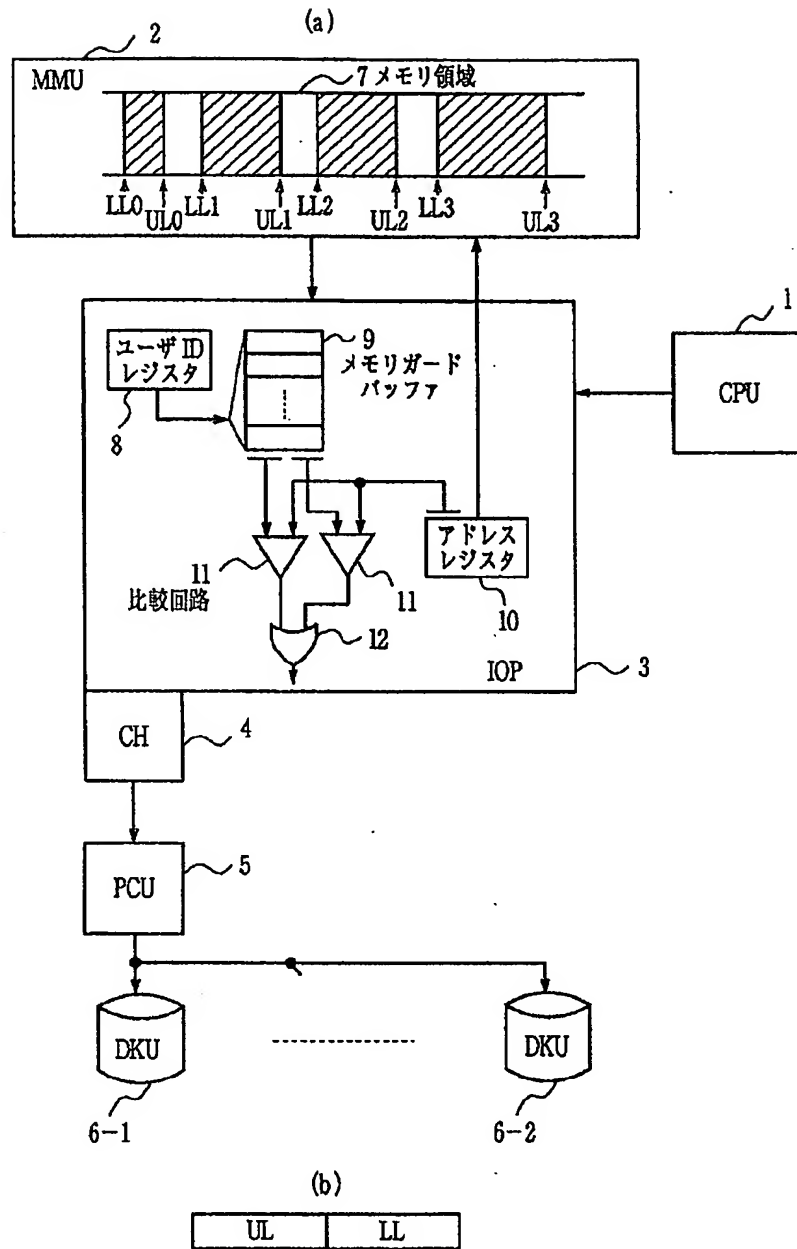
13

14

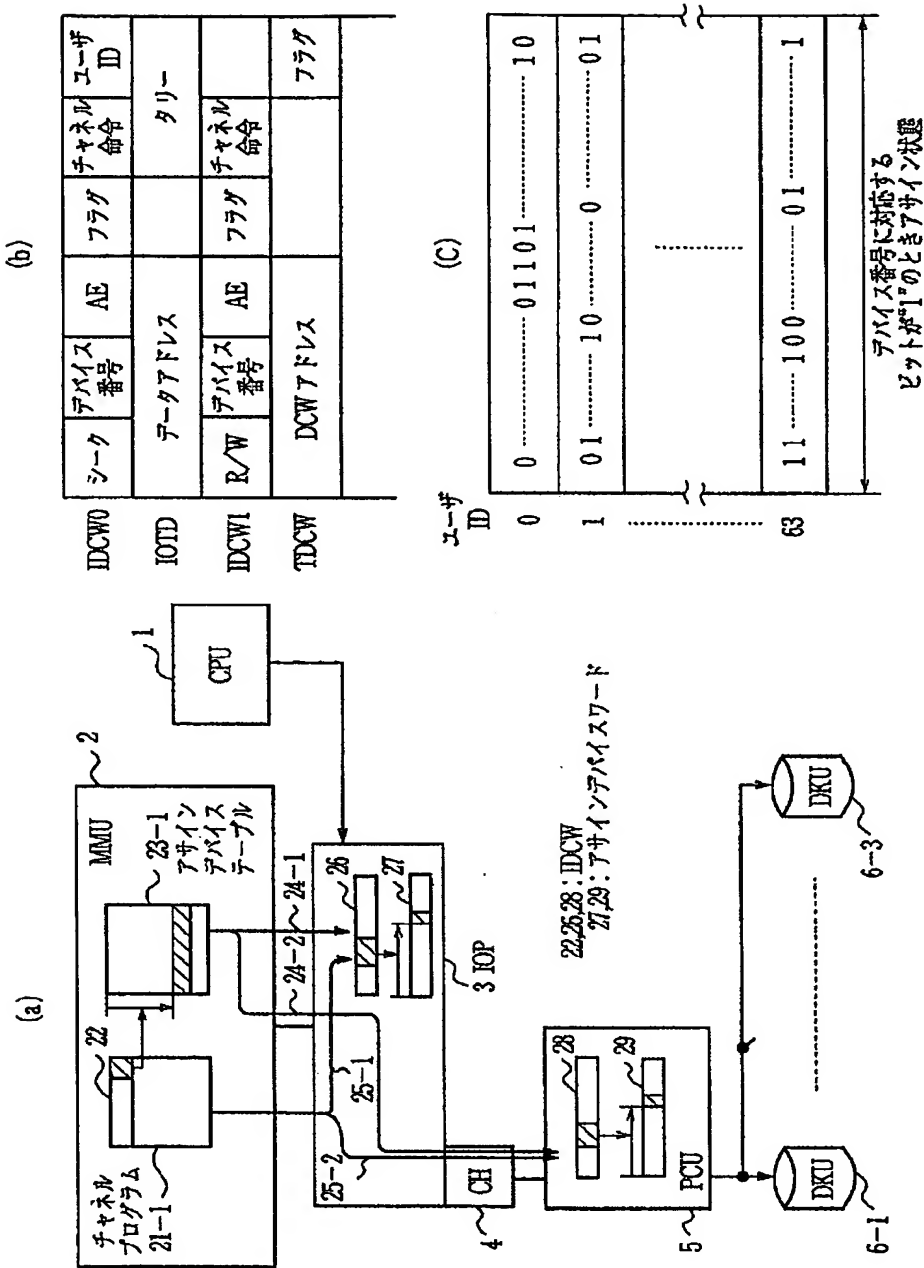
4 入出力チャネル (CH)
5 周辺制御装置 (PCU)
6-1, ~6-3 磁気ディスク装置 (DKU)
7, 61 メモリ領域
8 ユーザIDレジスタ
9, 63 メモリガードバッファ
10 アドレスレジスタ
11, 65 比較回路
12, 66 OR回路
21, 31, 41, 51 チャネルプログラム
22, 26, 28 IDCW
23 アサインデバイステーブル
24 アサインデバイスワード送出

25 IDCW送出
27, 29 アサインデバイスワード
32, 43, 53 シークデータ
33, 44 シリンダガードバッファテーブル
34 シリンダガードバッファテーブル転送
35 IDCW送出
36 IDCW
37 シリンダガードバッファ
42, 52 データエリア
10 54 ファイル
62 VMIDレジスタ
64 アドレスレジスタ

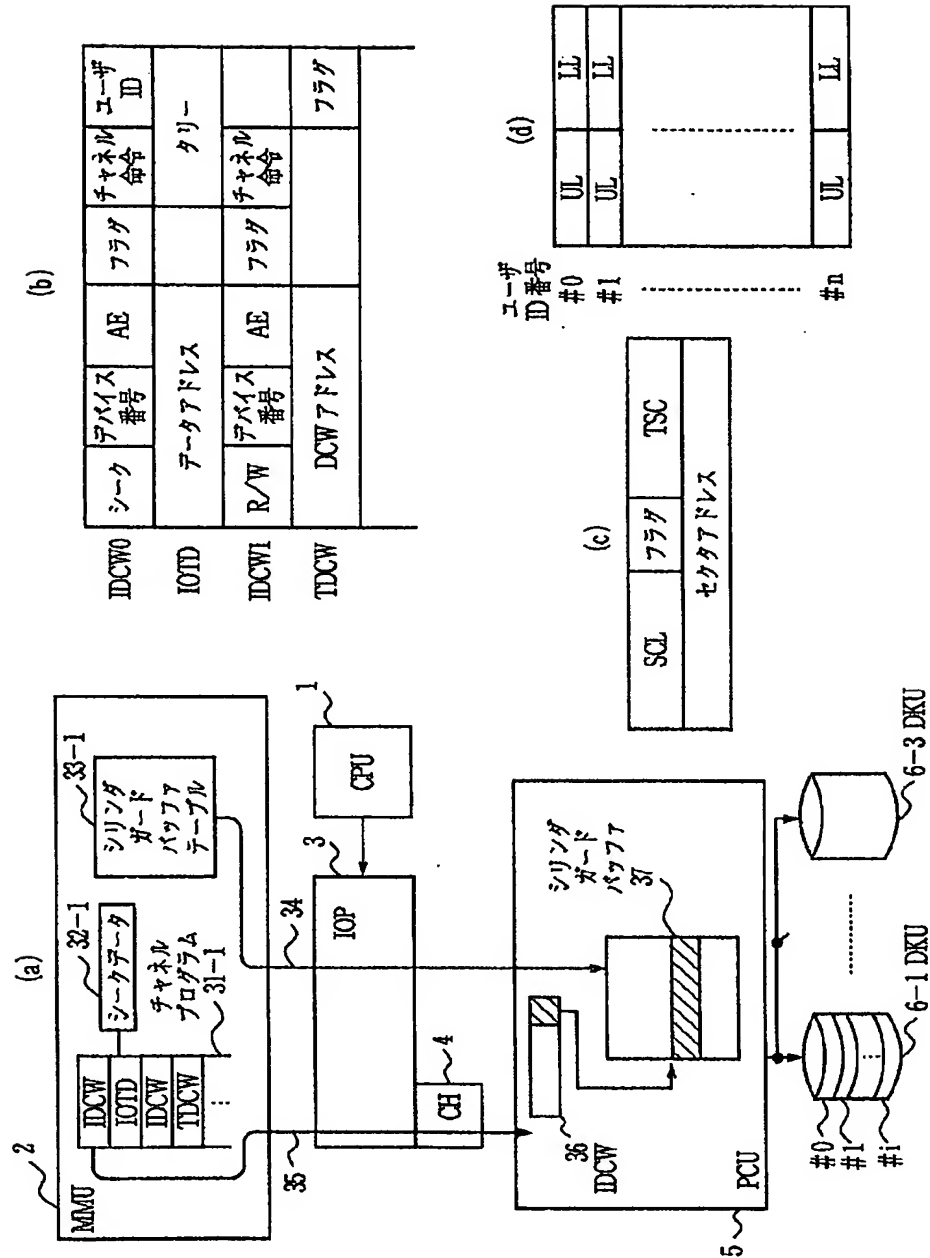
【図1】



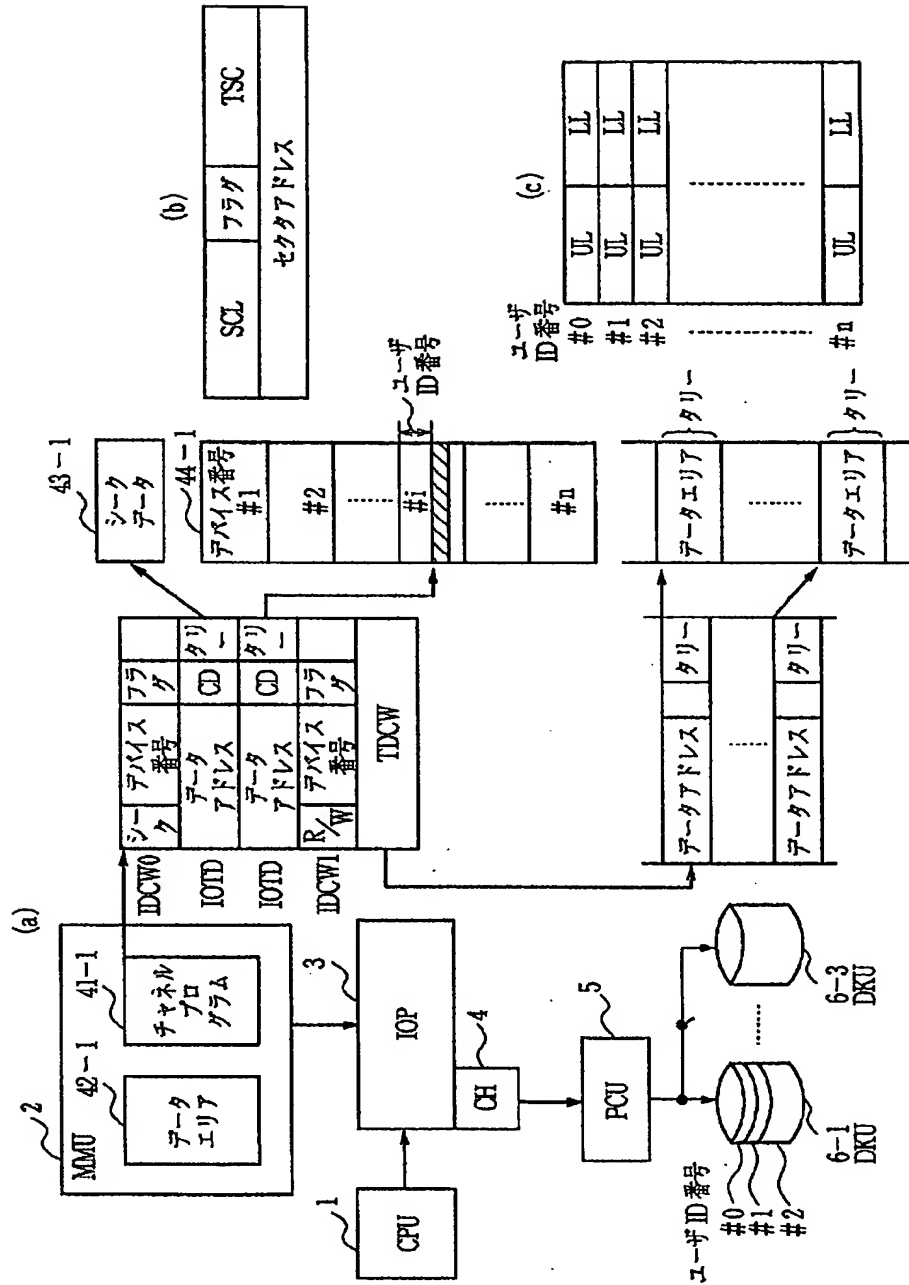
【図2】



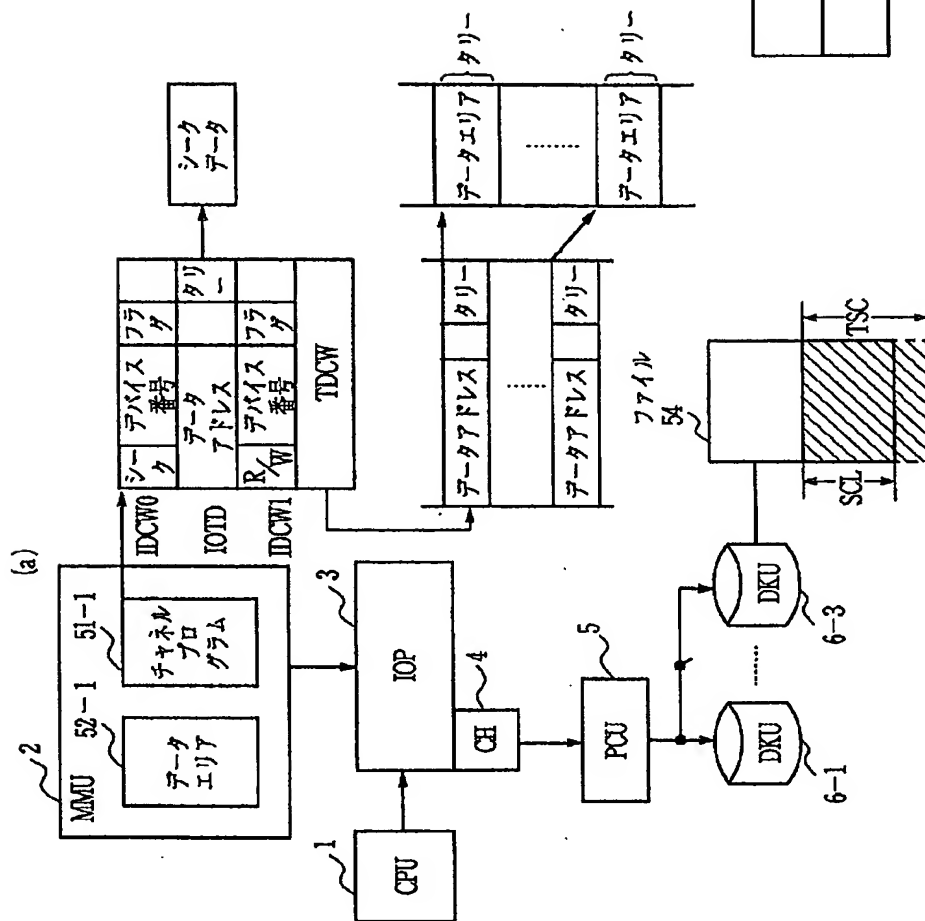
【図3】



【図4】



(b)	SOL	TSC
	セクタアドレス	



【図6】

